CLAIMS:

1. (Currently amended) A method, in a data processing system, for handling personally identifiable information, said method comprising:

providing, in a computer, a first set of object classes representing active entities in an information-handling process~~, wherein a limited number of privacy-related actions represent operations performed on data and wherein each of the active entities is a human being or legal entity~~;

providing, in said computer, a second ~~set of~~ object ~~classes~~ class representing ~~data~~ personally identifiable information and associated rules in said information-handling process~~, wherein at least one object class has said rules associated with said data, and wherein said data represents said personally identifiable information~~; and

processing transactions, in the data processing system, involving said personally identifiable information, using said computer and said first ~~and second~~ set of object classes and said second object class, so as to enforce a privacy policy, ~~associated with the personally identifiable information and defined by said rules, against one or more active entities represented by said first set of object classes, wherein each of the one or more active entities represented by said first set of object classes is a human being or legal entity.~~ wherein[[:]]

~~a first active entity represented by a first object class in said first set of object classes is a first data user that requests said personally identifiable information from a data subject that is a second active entity represented by a second object class in said first set of object classes,~~

~~said data subject is an active entity that is personally identifiable by said personally identifiable information[[;]]~~

~~a third active entity represented by a third object class in said first set of object classes is a second data user that requests said personally identifiable information from said first data user, and~~

said rules define if and how said personally identifiable information may be provided, by [[said]] a first data user that previously requested the personally identifiable information from an active entity that is personally identifiable by the personally

identifiable information, to [[said]] a second data user that requests said personally identifiable information from the first data user.

2. (Currently amended) The method of claim 1, wherein said first set of object classes include one or more object classes representing parties, selected from the group consisting of:

a data user object class,

a data subject object class,

a guardian object class, and

a privacy authority object class.

3. (Currently amended) The method of claim 1, wherein said ~~at least one~~ second object class, having said rules associated with said data, represents a filled paper form, including both collected data and rules regarding said collected data.

4-18. (Canceled)

19. (Previously Presented) The method of claim 1, further comprising:

transforming, based on said rules, said personally identifiable information into a depersonalized format prior to providing said personally identifiable information to the second data user.

20-22. (Canceled)

23. (New) The method of claim 1, wherein said privacy policy is associated with the personally identifiable information and defined by said rules, and is enforced against one or more active entities represented by said first set of object classes, and wherein each of the one or more active entities represented by said first set of object classes is a human being or legal entity.

24. (New) The method of claim 1, wherein:

a first active entity represented by a first object class in said first set of object classes is said first data user that previously requested said personally identifiable information from said data subject that is a second active entity represented by a second object class in said first set of object classes, and

a third active entity represented by a third object class in said first set of object classes is said second data user that requests said personally identifiable information from said first data user.

25. (New) The method of claim 19, wherein said transforming, based on said rules, said personally identifiable information into a depersonalized format prior to providing said personally identifiable information to the second data user comprises removing information that relates the personally identifiable information to the data subject in a reversible manner.

26. (New) The method of claim 1, further comprising:

transforming, based on said rules, said personally identifiable information into an anonymized format prior to providing said personally identifiable information to the second data user, wherein the anonymized format is a format in which all elements that may allow the personally identifiable information to be related to the data subject are stripped off in a non-reversible manner.

27. (New) An information handling system for handling personally identifiable information, said system comprising:

a processor; and

a memory coupled to the processor, wherein the memory comprises instructions which, when executed by the processor, cause the processor to:

provide a first set of object classes representing active entities in an information-handling process;

provide a second object class representing personally identifiable information and associated rules in said information-handling process; and

process transactions involving said personally identifiable information, using said first set of object classes and said second object class, so as to enforce a privacy policy, wherein said rules define if and how said personally identifiable information may be provided, by a first data user that previously requested the personally identifiable information from an active entity that is personally identifiable by the personally identifiable information, to a second data user that requests said personally identifiable information from the first data user.

28. (New) The system of claim 27, wherein the instructions further cause the processor to transform, based on said rules, said personally identifiable information into a depersonalized format prior to providing said personally identifiable information to the second data user.

29. (New) The system of claim 27, wherein said privacy policy is associated with the personally identifiable information and defined by said rules, and is enforced against one or more active entities represented by said first set of object classes, and wherein each of the one or more active entities represented by said first set of object classes is a human being or legal entity.

30. (New) The system of claim 27, wherein:

a first active entity represented by a first object class in said first set of object classes is said first data user that previously requested said personally identifiable information from said data subject that is a second active entity represented by a second object class in said first set of object classes, and

a third active entity represented by a third object class in said first set of object classes is said second data user that requests said personally identifiable information from said first data user.

31. (New) The system of claim 28, wherein said transforming, based on said rules, said personally identifiable information into a depersonalized format prior to providing said personally identifiable information to the second data user comprises removing

information that relates the personally identifiable information to the data subject in a reversible manner.

32. (New) The system of claim 27, wherein the instructions further cause the processor to transform, based on said rules, said personally identifiable information into an anonymized format prior to providing said personally identifiable information to the second data user, wherein the anonymized format is a format in which all elements that may allow the personally identifiable information to be related to the data subject are stripped off in a non-reversible manner.

33. (New) A computer program product comprising a computer-usable medium having computer-executable instructions for handling personally identifiable information, wherein said computer-executable instructions, when executed by a computing device, cause the computing device to:

provide a first set of object classes representing active entities in an information-handling process;

provide a second object class representing personally identifiable information and associated rules in said information-handling process; and

process transactions involving said personally identifiable information, using said first set of object classes and said second object class, so as to enforce a privacy policy, wherein said rules define if and how said personally identifiable information may be provided, by a first data user that previously requested the personally identifiable information from an active entity that is personally identifiable by the personally identifiable information, to a second data user that requests said personally identifiable information from the first data user.

34. (New) The computer program product of claim 33, wherein the instructions further cause the processor to transform, based on said rules, said personally identifiable information into a depersonalized format prior to providing said personally identifiable information to the second data user.

35. (New) The computer program product of claim 33, wherein said privacy policy is associated with the personally identifiable information and defined by said rules, and is enforced against one or more active entities represented by said first set of object classes, and wherein each of the one or more active entities represented by said first set of object classes is a human being or legal entity.

36. (New) The computer program product of claim 33, wherein:

a first active entity represented by a first object class in said first set of object classes is said first data user that previously requested said personally identifiable information from said data subject that is a second active entity represented by a second object class in said first set of object classes, and

a third active entity represented by a third object class in said first set of object classes is said second data user that requests said personally identifiable information from said first data user.

37. (New) The computer program product of claim 34, wherein said transforming, based on said rules, said personally identifiable information into a depersonalized format prior to providing said personally identifiable information to the second data user comprises removing information that relates the personally identifiable information to the data subject in a reversible manner.

38. (New) The computer program product of claim 33, wherein the instructions further cause the processor to transform, based on said rules, said personally identifiable information into an anonymized format prior to providing said personally identifiable information to the second data user, wherein the anonymized format is a format in which all elements that may allow the personally identifiable information to be related to the data subject are stripped off in a non-reversible manner.